

United States District Court

EASTERN DISTRICT OF VIRGINIA

Richmond Division

UNITED STATES OF AMERICA

v.

CRIMINAL COMPLAINT

CASE NUMBER:

3:13mJ028

DAWDA DRAMMEH

I, the undersigned complainant, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

On or about April 15, 2012 in the Eastern District of Virginia, the defendant did

knowingly, with intent to defraud, and in a manner affecting interstate and foreign commerce, possess fifteen or more unauthorized and counterfeit access devices

in violation of Title(s) 18 United States Code, Section(s) 1029(a)(3).

I further state that I am a(n) Special Agent, U.S. Secret Service and that this complaint is based on the following facts:

Official Title

SEE ATTACHED AFFIDAVIT

REVIEWED AND APPROVED:



Michael C. Moore
Assistant United States Attorney

Continued on the attached sheet and made a part hereof:



Yes



No



Matthew Halin, Special Agent
U.S. Secret Service

Sworn to before me and subscribed in my presence,

Date

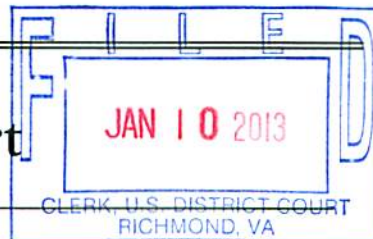
January 10, 2013

at

Richmond, Virginia
City and State

Name & Title of Judicial Officer

Signature of Judicial Officer David J. Novak
United States Magistrate Judge



**AFFIDAVIT IN SUPPORT OF APPLICATION FOR CRIMINAL COMPLAINT
AND ARREST WARRANT**

I, Matthew Paul Halin, being duly sworn, depose and say:

INTRODUCTION

1. I am a Special Agent with the United States Secret Service. I have been employed as a Special Agent since 2011, and I am currently assigned to the Office of Investigations, Richmond Field Office. I have investigated access device fraud cases. I have participated in the preparation and presentation of arrest warrants and search warrants, and I am familiar with the methods of individuals who commit offenses related to manufacturing, using, and possessing fraudulent access devices.

2. This affidavit is in support of an arrest warrant for Dawda Drammeh, whose last known address, 8711 Glenarden Parkway, Glenarden, Maryland 20706 ("Subject Premises"), is situated in the Southern District of Maryland.

3. I have conducted this investigation with assistance from several other law enforcement officers including Special Agents of the U.S. Secret Service ("USSS"), a Trooper of the Virginia State Police ("VPS"), and a Special Agent of the Virginia State Police. This affidavit is based upon my personal knowledge, my conversations with other law enforcement agents and sources upon interviews, and upon my examination of various transcripts, reports, and other records. When the contents of documents or statements of others are reported herein, they are reported in substance and part unless otherwise indicated.

4. Because this affidavit is being submitted for the limited purpose of securing an arrest warrant for Dawda Drammeh, I have not included each and every fact known to me

concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that Dawda Drammeh committed violations of 18 U.S.C. § 1029, including, but not limited to, 18 U.S.C. § 1029(a)(3) (possession of 15 or more unauthorized or counterfeit access devices).

5. As a result of the initial investigation, described more fully below, there is probable cause to believe that Dawda Drammeh committed violations of federal law, 18 U.S.C. § 1029, including, but not limited to, 18 U.S.C. § 1029(a)(3) (possession of 15 or more unauthorized or counterfeit access devices).

PERTINENT FEDERAL CRIMINAL STATUTES

This investigation concerns alleged violations of 18 U.S.C. § 1029, relating to access device fraud. Title 18 U.S.C. § 1029 prohibits a person from knowingly and with intent to defraud producing, using or trafficking in counterfeit or unauthorized access devices or device-making equipment, or possessing 15 or more counterfeit or unauthorized access devices.

DETAILS OF THE INVESTIGATION

Initiation of Investigation

1. On 10/19/2012, the U.S. Secret Service Richmond Field Office was contacted by the Virginia State Police advising one individual, identified as Dawda Drammeh, was in custody with VSP as a result of an arrest warrant. Drammeh was arrested for violations of Virginia Code 18.2-192 (Credit Card Theft) as a result of a traffic stop conducted by the VSP on April 15, 2012. During the traffic stop, Drammeh was found to not have a valid driver's license and giving a false name to the VSP. Drammeh was arrested for driving without a license and giving a false name to a law enforcement officer. The vehicle, a

grey 2005 Acura Sedan with Vehicle Identification Number: VIN:19UUA66295A033009 was towed to a VSP facility. VSP conducted an inventory search of the vehicle pursuant to their department policy. The search revealed approximately thirty six pre-paid gift / debit cards (device 1), a laptop computer (device 2), card reader (device 3) and an iPad.

Examination of Subject Cards

2. On 7/20/2012, a USSS preliminary examination for the Bank Identification Number (BIN) of the subject cards revealed the authentic account numbers and the issuing banks. This information was contained on the magnetic stripe of the cards which provided the track information. Many of the subject cards were re-encoded with account numbers not associated with the actual subject cards. Based on my training and experience, this re-encoding is consistent with an illegal identity theft scheme. In fact, I am unaware of any legitimate reason for why magnetic stripes on subject cards such as the ones examined would be encoded with account numbers not associated with those accounts. The accounts on the subject cards were issued by several banks to include;;

BANK	LAST FOUR OF ACCT # (Individual Cards)
American Express	1002
Bank of America	9116
Chase Bank	1614, 2560, 4010, 4688
Citibank	6516, 0539, 8245
Comerica Bank	5502
East Boston Savings Bank	8535
FIA Card Services	0463, 7100
Liberty Bank	2573
Sovereign Bank	2464
U.S. Bank National Association	6496, 3321
USAA	2312
Wells Fargo Bank	4830, 6652, 7823, 6072, 3260, 1181, 8981, 9830, 8139, 8809, 8800, 0828,

6250, 1499, 2930, 7507, 9917, 1417

Interview of Drammeh

3. On 10/19/2012, an agent of the USSS, Richmond Field Office, and a Trooper of the VSP interviewed Drammeh at the Richmond Field Office. When asked to describe his involvement with the re-encoded cards, Drammeh stated that he had knowledge of the manufacturers, distributors and criminal organization in connection with the cards.

Drammeh described himself as a middle man for the organization and is able to obtain cards and identifications for other individuals. When asked how the cards were used to commit fraud, Drammeh advised that an embossed credit card would be sold for \$25 and the account number for \$50. He stated that there would be a 50/50 split in proceeds between the manufacturer and the individual (shopper) who would be making the purchases. Shoppers would make purchases of merchandise at various stores and would either make a return at a later date for a cash refund or would sell the merchandise online. Drammeh stated that individuals are using cards in Virginia, North Carolina, Georgia and New York.

4. Following the conclusion of the interview, consent was given by Drammeh to the VSP and USSS to conduct a search of his rental vehicle. Drammeh stated that the only contraband in the vehicle was marijuana located in a pack of cigarettes. The search revealed a small amount of marijuana and nine gift / credit cards. Three of the cards were embossed with the VISA logo, but were encoded with Discover Bank account numbers, which had fraudulent transactions associated with the accounts.

Examination of Subject Computer

5. On 8/31/12 a search warrant was executed on the Sony Vaio laptop (device 2). An agent of the USSS, Richmond Field Office conducted a forensic examination of device 2, which resulted in approximately fifty eight authentic account numbers and the issuing banks. The accounts on the subject laptop were issued by several banks to include;

BANK	LAST FOUR OF ACCT # (Individual Cards)
American Express	4000, 9916, 3512, 7532, 7600
Armed Forces Bank	8131, 0319
Asheville Savings Bank, S.S.B.	4659
Banco Popular, North America	8033
Discover Bank	7394, 4686, 7911, 2294, 8429, 9568, 1048, 3523, 3779, 4204, 3363, 8350, 2337, 6136, 1064

Not an inclusive list

Results of Examination of Equipment and Devices found in Drammeh's Vehicle

6. A USSS examination of the Sony Vaio Laptop Computer (Device 2) and card reader (Device 3) revealed these are similar instruments used in re-encoding credit/debit/gift cards with magnetic stripes to contain authentic account holder information issued by legitimate banks. The process of re-encoding subject cards with magnetic stripes with unauthorized legitimate account holder information is described as follows:

DEFINITIONS

Based on my training and experience, I use the following technical terms to convey the following meanings:

The term “**computer**” or “**laptop**” as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as “an electronic, magnetic, optical electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”

The terms “**skimming**,” “**skimming device**,” and “**skimmer**,” refer to the act of or the device used for the copying or encoding of electronically transmitted full track data on the magnetic strip of a credit card, to enable valid electronic payment authorization to occur between a merchant and the issuing financial institution. A skimmer is the slang term for a device used to read and record the magnetic code(s) from a credit card. These devices have the capability of storing the recorded information, which can later be used for fraudulent purposes. A skimming device is often used to read, store and encode account information on counterfeit cards or to re-encode genuine cards with an unauthorized account number to make fraudulent withdrawals or conduct other unauthorized transactions.

Access device, as used herein, is defined in Title 18 U.S.C. § 1029(e)(1) as “any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment or instrument identifier or other means of account access that can be used, alone or in

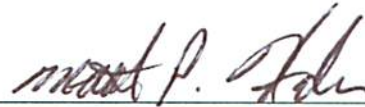
conjunction with another access device, to obtain money, goods, services or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer initiated solely by paper instrument).”

7. Based on my training, experience, and research, I know that the items identified as collectively as “Device 1” have capabilities that allow them to be used as “access devices” to obtain money, goods, services or any other thing of value, or can be used to initiate a transfer of funds. Based on my training and experience, Device 2 has capabilities that allow it to serve as a storage device and to facilitate the re-encoding of magnetic stripes. Based on my training, experience, and research, I know that Device 3 is a skimmer with the capability to read, encode and record the magnetic code(s) from a credit card (for future fraudulent use). The stolen data/information captured through the use of this type of device can be stored on this device, transferred to a computer, and later retrieved so that said data/information can be re-encoded on counterfeit, genuine debit /credit/gift cards, or counterfeit cards for the purpose of future fraudulent use.

CONCLUSION

Based upon the facts described throughout this affidavit, I respectfully submit that there is probable cause to believe that Dawda Drammeh knowingly and with intent to defraud is producing, using or trafficking in counterfeit or unauthorized access devices or device-making equipment.

I therefore respectfully request that this Court issue a criminal complaint charging Dawda Drammeh with a violation of 18 U.S.C. § 1029(a)(3) (possession of 15 or more unauthorized or counterfeit access devices) as well as a warrant authorizing his arrest on that complaint.



Matthew Paul Halin
Special Agent
United States Secret Service

Sworn to and subscribed before me on January 10th, 2013.

/s/ [Signature]
David J. Novak
United States Magistrate Judge

David J. Novak
United States Magistrate Judge